PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-073311

(43)Date of publication of application : 16.03.1999

(51)Int.Cl. G06F 9/06
G06F 9/445
G06F 12/14

(21)Application number : 09-234945

(22)Date of filing : 29.08.1997

(71)Applicant : VERCON LTD

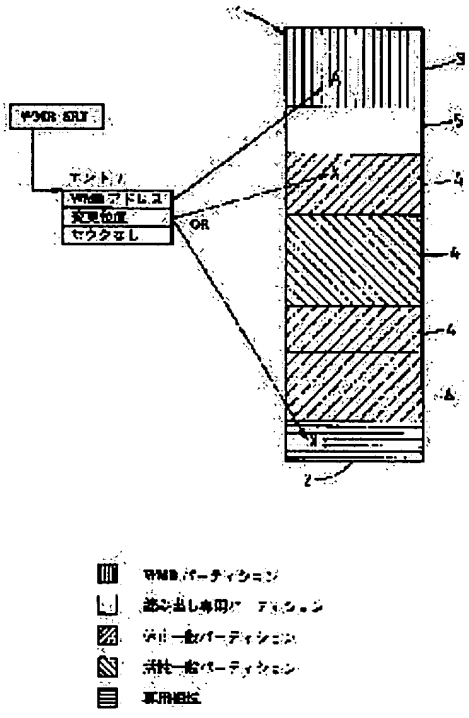
(72)Inventor : NORMAN JACKSON WHITE
DAVID ROBB
REGINALD KILLIAN

(54) METHOD AND DEVICE FOR CONTROLLING ACCESS AND CHANGE OF INFORMATION STORED IN RECORDING MEDIUM IN COMPUTER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and device for controlling the access and change of information stored on a recording medium forming a part of a computer system.

SOLUTION: Information stored on the recording medium is divided into plural unoverlapped partitions including boot partitions and at least one general partition. One of plural partitions is specified as a write-many-read-many (WMR) partition, and if a write command is issued to overwrite the remaining information stored in one partition or the WMR partition by updating information, optional remining information is stored so as to access updating information in accordance with a request in a remaining cession and the updating information is written in a position other than a position in which a virtual pointer for the updating information is set up or stored.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－73311

(43)公開日　平成11年(1999)３月16日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｚ
	9/445			12/14	３１０Ａ
	12/14	３１０		9/06	４２０Ｇ

審査請求　未請求　請求項の数30　ＯＬ　（全 16 頁）

(21)出願番号　特願平9－234945

(22)出願日　平成９年(1997)８月29日

(71)出願人　597124305
パーコン　リミテッド
イギリス国エディンバラ，キャッスル　テラス　20，サルタイア　コート，レベル　2，シェファード　アンド　ウェッダーバーン　気付

(72)発明者　ノーマン　ジャクソン　ホワイト
イギリス国キンロス　ミュアーズ　96，”ザ　デル”

(72)発明者　デビッド　ロップ
イギリス国カークカルディ，ファーム　コッテージズ，パルウェリー　1

(74)代理人　弁理士　浅村　皓　（外３名）

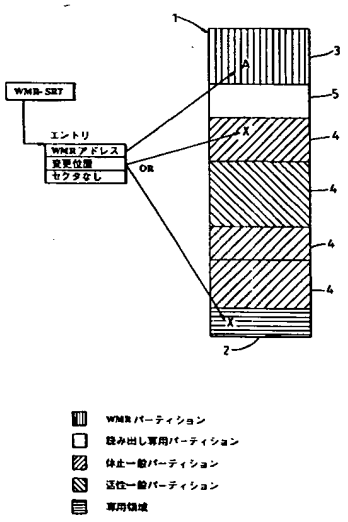
最終頁に続く

(54)【発明の名称】　コンピュータ・システムにおける記憶媒体に記憶された情報のアクセス及び変更を制御する方法及び装置

(57)【要約】

【課題】　コンピュータ・システムの一部を形成する記憶媒体に記憶される情報のアクセス及び変更を制御する方法及び装置を提供する。

【解決手段】　前記記憶媒体に記憶された情報をブート・パーティション及び少なくとも一つの一般パーティションを含む重複しない複数のパーティションに分割し、前記パーティションのうちの一つを多数回復可能書き込みに指定し、もし書き込みコマンドが更新情報により一つの又は前記ＷＭＲパーティションに記憶されている残留情報に重ね書きするように発行されたときは、残りのセッション中の要求に従って前記更新情報をアクセスできるように、任意の残留情報が記憶され、かつ前記更新情報に対する（仮想）ポインタが設定又は保持されている位置以外の位置に、前記更新情報を書き込む。



【特許請求の範囲】
【請求項１】　コンピュータ・システムの一部を形成する記憶媒体上に記憶した情報のアクセス及び変更を制御する方法であって、
前記記憶媒体に記憶された情報をブート・パーティション及び少なくとも一つの一般パーティションを含む重複しない複数のパーティションに分割することを含む方法において、
前記パーティションのうちの一つを多数回復可能書き込み（ＷＭＲ）パーティションに指定し、もし書き込みコマンドが更新情報により一つの又は前記ＷＭＲパーティションに記憶されている残留情報に重ね書きするように発行されたときは、残りのセッション中の要求に従って前記更新情報をアクセスできるように、任意の残留情報が記憶され、かつ前記更新情報に対する（仮想）ポインタが設定又は保持されている位置以外の位置に、前記更新情報を書き込むことを特徴とするコンピュータ・システムの一部を形成する記憶媒体に記憶したアクセス及び変更を制御する方法。
【請求項２】　システム・リセットが前記更新情報をこの情報に対するポインタのリストと共にクリアさせることにより、前記ＷＭＲパーティションをそのオリジナルの状態に戻す請求項１記載の方法。
【請求項３】　前記記憶媒体上のブート・パーティションはＷＭＲパーティションを指定している前記いずれかの請求項記載の方法。
【請求項４】　一般パーティションがＷＭＲパーティションを指定している前記いずれかの請求項記載の方法。
【請求項５】　前記コンピュータ・システムの中央処理装置（ＣＰＵ）から独立し、かつそのユーザにアクセス不能にされたスーパバイザ手段（スーパバイザ）が設けられ、
前記管理手段は、セクタから読み出されるか又はセクタに書き込まれる情報がオペレーティング・システム情報であるか又はユーザ情報であるか、前記セクタが前記ブート・パーティションにあるか又は一般パーティションにあるか、及び前記パーティションは活性であるか又は不活性であるかに従って、前記記憶媒体上での読み出し／書き込み動作を許可し、規制し、又は禁止し、
前記管理手段は、活性な一般パーティション上でのみのフォーマット動作を許可し、かつ前記ブート・パーティション上で又は不活性な一般パーティション上でフォーマット動作を禁止し、
かつ、禁止された読み出し、書き込み又はフォーマット動作を実行したときはユーザに警告を発生する前記いずれかの請求項記載の方法。
【請求項６】　専用領域と呼ばれるスーパバイザによってのみアクセスされる前記記憶媒体上で空間を確保する請求項５記載の方法。
【請求項７】　前記専用領域は特殊パーティション、前記ＷＭＲパーティション内のある範囲のセクタ、又は休止パーティション内の未割り付けセクタである請求項６記載の方法。
【請求項８】　各ＷＭＲパーティションは、これに関連したセクタ再割り付けテーブル（ＳＲＴ）を有し、前記テーブルを前記スーパバイザのランダム・アクセス・メモリ（ＲＡＭ）に保持し、ＳＲＴにおける各エントリは更新されたＷＭＲパーティションにおけるある範囲のセクタのアドレスと、前記更新情報が位置するアドレスと、前記更新情報を位置決めするアドレスとを定義し、その位置が前記専用領域内にある前記いずれかの請求項記載の方法。
【請求項９】　コンピュータ・システムの記憶媒体に記憶された情報に対するアクセス及び変更を制御する装置が設けられ、前記記憶媒体はブート・パーティション及び少なくとも一つの一般パーティションを含む複数の非重複パーティションに分割された装置において、
前記パーティションのうちの少なくとも一つは多数回復可能書き込み（ＷＭＲ）を備え、使用中に、もし書き込みコマンドが前記ＷＭＲパーティションに記憶されている任意の情報に重ね書き（更新）するように発行されたときは、残りのセッション中の要求に従って前記更新情報をアクセスするように、前記更新情報を前記記憶媒体上の他の位置に記憶し、かつ前記更新情報に対する（仮想）ポインタを保持し、システム・リセットは前記更新情報を前記更新情報に対するポインタのリストと共にクリアさせることを特徴とする装置。
【請求項１０】　前記装置は、前記コンピュータ・システムの中央処理装置（ＣＰＵ）から独立し、かつユーザにアクセス不能にされたスーパバイザ手段（スーパバイザ）を備え、
前記管理手段は、セクタから読み出される又はセクタに書き込まれる情報がオペレーティング・システム情報であるか又はユーザ情報であるか、前記セクタが前記ブート・パーティションであるか又は一般パーティションであるか、及びもし前記パーティションが一般パーティションであれば、前記パーティションは活性であるか又は不活性であるかに従って、前記記憶媒体上での読み出し及び書き込み動作を許可し、規制し、又は禁止し、
前記管理手段は、更に、活性となる一般パーティション上のみでのフォーマット動作を許可し、かつ前記ブート・パーティション上又は不活性な一般パーティション上でのフォーマット動作を禁止し、
前記監視手段は、禁止された読み出し、書き込み又はフォーマット動作であって、前記スーパバイザにより阻止されている前記動作を実行するための試行をしたのであれば、ユーザに警告を発生させる請求項９記載の装置。
【請求項１１】　コンピュータ・システムの一部を形成する記憶媒体上に記憶された情報に対するアクセス及び変更を制御する方法であって、

前記記憶媒体上に記憶された情報をブート・パーティション及び少なくとも一つの一般パーティションを含む複数の非重複パーティションに分割する方法において、
前記パーティションのうちの少なくとも一つを多数回復可能書き込み（WMR）に指定し、使用中に、もし書き込みコマンドを実行する前に、前記書き込みコマンドがある又は前記WMRパーティションに記憶されている任意の情報に重ね書きするように発行された場合に、要求されたとき、例えばシステム・リセットのときに、前記情報を前記記憶媒体上の他の位置にコピーすると共に記憶して前記WMRパーティションにコピーして復帰させることを特徴とする方法。

【請求項12】　前記コンピュータ・システムの中央処理装置（CPU）から独立して、セクタ内に記憶された情報の型式、及び前記セクタが配置されている前記パーティションの型式及びステータスに従って動作を許可する、規制する又は阻止するように、前記記憶媒体に記憶された情報に基づく読み出し、書き込み及びフォーマット動作の実行を制御する管理手段（スーパバイザ）を備え、
前記監視手段は、禁止された読み出し、書き込み又はフォーマット動作を実行するために試行したのであれば、前記コンピュータ・システムのリセットを要求させて、前記リセットはメモリをクリアさせ、かつオペレーティング・システムをロードさせる請求項11記載の方法。

【請求項13】前記記憶媒体は、特殊パーティション（ウイルス隔離空間）を備え、各WMRパーティションはファイル割り付けテーブル（FAT）が割り付けられ、このテーブルは前記特殊パーティションに保持され、FATにおける各エントリは前記WMRパーティションにおいて変更されたクラスタのアドレス、及び前記クラスタにオリジナルに保持された前記情報のコピーの前記アドレスを定義する請求項11又は請求項12記載の方法。

【請求項14】　前記クラスタにオリジナル保持された情報は前記特殊パーティションにコピーされる請求項13記載の方法。

【請求項15】　前記クラスタにオリジナルに保持された前記情報は不活性パーティションにコピー可能にされている請求項13記載の方法。

【請求項16】　コンピュータ・システムの記憶媒体に記憶された情報に対するアクセス及び変更を制御する装置であって、前記記憶媒体はブート・パーティション及び少なくとも一つの一般パーティションを含む複数の非重複パーティションに分割されている装置において、
前記パーティションのうちの少なくとも一つは多数回復可能書き込み（WMR）パーティションを備え、使用において、もし書き込みコマンドが前記書き込みコマンドを実行する前に、一つの又は前記WMRパーティションに記憶された任意の情報を重ね書きするように発行されたときは、前記情報はコピーされると共に前記記憶媒体のどこかに記憶されて、必要なときに、例えばシステム・リセットにより、前記WMRパーティションにコピーにより戻されることを特徴とする装置。

【請求項17】　前記コンピュータ・システムの中央処理装置（CPU）から独立し、セクタ内に記憶された情報の型式と、前記セクタが配置されている前記パーティションの型式及びステータスに従って動作を許可する、規制する又は阻止するように、前記記憶媒体上に記憶された読み出し、書き込み又はフォーマット動作の実行を制御する監視手段（スーパバイザ）を備え、使用において、前記監視手段は、禁止された読み出し、書き込み又はフォーマット動作を実行するために試行されたならば、前記コンピュータ・システムのリセットを要求させる請求項16記載の装置。

【請求項18】　読み出し動作が前記ブート・パーティションにおける任意の情報について許可され、前記ブート・パーティションに対する書き込み又はフォーマットの試行がシステム・リセットを発生させる請求項1又は11記載の方法。

【請求項19】　前記記憶媒体の複数のブート・セクタは、前記記憶媒体オペレーティング・システムにより定義可能とされる前記ブート・パーティションの開始セクタの位置に無関係に、前記ブート・パーティションの一部であるとみなされる請求項18記載の方法。

【請求項20】　活性な一般パーティションにおける任意のオペレーティング・システム情報セクタ又はユーザ発生の情報セクタの読み出しが許可され、このようなユーザ発生の情報セクタに対する書き込みが許可され、かつこのようなオペレーティング・システムの情報セクタに対する書き込みが前記パーティションの大きさ及び境界を変更するための試行がシステム・リセットを発生させるように、規制される請求項18又は19記載の方法。

【請求項21】　不活性な一般パーティションのオペレーティング・システム・セクタから情報を読み出すことのみが許可され、このようなパーティション上の他の読み出し、書き込み又はフォーマット動作を実行するための試行は、否定できるようにされる、又はシステム・リセットを発生させる請求項18又は19記載の方法。

【請求項22】　読み出し、書き込み及びフォーマット動作の実行の規制又は阻止は、前記記憶媒体のセット・アップ又は保守できるように解除され、かつその後に再復帰可能にされている請求項21記載の方法。

【請求項23】　前記記憶媒体はハード・ディスク、フロッピー・ディスク、光ディスク又はテープのうちの一つから選択可能にされている請求項1又は11記載の方法。

【請求項24】　前記記憶媒体はファイルサーバであり、前記コンピュータ・システムはローカル・エリア・

ネットワークであり、かつユーザ・コンピュータにより禁止された動作を実行するための試行が前記ユーザ・コンピュータのリセットを発生させるように、そのユーザ・コンピュータが前記ファイルサーバのどのパーティションを決定できるのかを使用している請求項1又は11記載の方法。

【請求項25】　前記コンピュータ・システムに関連するように適応されたハードウエア手段を備えている請求項11又は16記載の装置。

【請求項26】　前記装置は前記コンピュータ・システムに関連するように適応されたハードウエア手段を備えている請求項9又は16記載の装置。

【請求項27】　前記装置はハードウエア手段とファームウエアとの組み合わせを備え、両者は前記コンピュータ・システムに関連するように適応されている請求項9又は16記載の装置。

【請求項28】　ユーザに対して及びどのようなウイルスに対してもアクセス不能にされ、かつ前記記憶媒体又はその制御のもとに置かれた記憶媒体の副分割の間における及びその副分割内における全てのデータ転送を監視するプロセッサを備え得る請求項9、10、16又は17記載の装置。

【請求項29】　ウイルス隔離空間にパスワードを入力して記憶させ、前記パスワードがその後にアンスーパバイズド・モードに対するアクセスを許可するように使用可能にされている請求項1又は11記載の方法。

【請求項30】　前記ユーザは、新しいセッションの開始で変更されたファイル（又は複数のファイル）を一つ又は前記WMRパーティション（又は前記複数のWMRパーティション）に記憶された前記情報を置換できるように、シャットダウン前に、活性パーティションにおける前記変更ファイルを記憶するバッチ・ファイル（又は複数のバッチ・ファイル）を作成可能にされている請求項1から8まで、又は請求項11のいずれかに記載された方法。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】本発明は、コンピュータ・システムにおける情報に対するアクセス及びその汚損を制御する方法及び装置に関する。

【0002】

【従来の技術】本発明者によるPCT／GB91／00261（WO91／13403）（ここではその内容を引用により関連させる。）も特にコンピュータ・システム内の「ウイルス」プログラムのような敵対的なプログラムの検出及び包含に関する方法及び装置を開示している。この文書では、記憶媒体に記憶された情報をブート・パーティション及び複数の一般パーティションを含む重複しない複数のパーティションに分割すると共に、各パーティションが更に複数のセクタに分割され、前記コンピュータ・システムが使用中の与えられた時点で、前記一般パーティションの指定された任意のサブセットが活性であるコンピュータ・システムの一部を形成する記憶媒体に記憶した情報に対するアクセス及び変更を制御する方法（及び関連する装置）において、前記コンピュータ・システムの中央処理装置（CPU）から独立し、かつユーザにアクセス不能にされて、前セクタ内に記憶された情報の型式、及び前記セクタが配置されているパーティションの型式及びステータスに特に従って動作を規制又は阻止ができるように、前記記憶媒体上に記憶された情報に基づく読み出し、書き込み及びフォーマット動作の実行を制御する管理手段（スーパバイザ）を備え、前記管理手段は、禁止された読み出し、書き込み又はフォーマット動作を実行するために試行したのであれば、前記コンピュータ・システムのリセットを要求させ、前記リセットがメモリをクリアさせ、かつオペレーティング・システムをロードさせることにより特徴付けられた方法（及び関連する装置）が開示されている。

【0003】PCT／GB91／00261において開示された発明において、ブート・パーティションは、システムがスーパバイズド・モードのときに、「読み出し専用」となる。これは、DOSユティリティ及びプログラムが自己変更するものでない限り、これらの実行を許可している間のウイルスによる攻撃を阻止している。

【0004】

【発明が解決しようとする課題】PCT／GB91／00261によるウイルス隔離の概念以後、PCオペレーティング・システムに対する変更及び改良がなされた。これらはウイルス隔離発明の範囲に一定の限界が存在する。例えば、

（1）マイクロソフト・ウィンドウズは、厳密には自己変更するものでなくとも、ウィンドウズ・ディレクトリ内に置かれた一定の複数ファイルを書き込めることを必要とする。

（2）システム・アドミニストレータは、それが自己変更であることを認識することなく、ブート・パーティションに実行可能な内容をインストールできる。このように実行可能な内容がブート・パーティションにインストールされると、このプログラムの自己変更は、システムがスーパバイズド・モードのときに試行され、スーパバイザは書き込み試行を阻止し、かつシステムを凍結させる。

（3）マイクロソフト・ウィンドウズの仮想メモリ・マネジャーはウィンドウズのディレクトリ及びブート・パーティションのルート・ディレクトリのうちのいずれか、又は両方に対する書き込みアクセスを必要とすることがある。

（4）ネットワーク・ソフトウェアはブート・パーティションに対するアクセスを必要とすることがある。

（5）一般に、複雑なオペレーティング・システムによ

り、ブート・パーティションを「読み出し専用」にすることは限定的であり、互換性をなくし、かつ高い管理オーバヘッドの原因となり得る。

【0005】

【課題を解決するための手段】本発明の目的は、前述の問題を除去又は軽減することである。

【0006】本発明の第1の特徴によれば、コンピュータ・システムの一部を形成する記憶媒体に記憶したアクセス及び変更を制御する方法であって、記憶媒体に記憶された情報をブート・パーティション及び少なくとも一つの一般パーティションを含む重複しない複数のパーティションに分割することを含む方法において、前記パーティションのうちの一つを多数回復可能書き込み（Ｗｒｉｔｅ　Ｍａｎｙ　Ｒｅｃｏｖｅｒｂｌｅ：WMR）に指定し、もし書き込みコマンドが更新情報により、一つの又は前記WMRパーティションに記憶されている残留情報に重ね書きするように発行されたときは、残りのセッション中の要求に従って前記更新情報をアクセスできるように、前記又は任意の残留情報が記憶され、かつ前記更新情報に対する（仮想）ポインタが設定又は保持されている位置以外の位置に、前記更新情報を書き込むことを特徴とするコンピュータ・システムの一部分を形成する記憶媒体に記憶したアクセス及び変更を制御する方法が提供される。

【0007】システム・リセットが前記更新情報をこの情報に対するポインタのリストと共にクリアさせる。これは非スーパバイズド・モードにより構築された際にWMRパーティションをそのオリジナルの状態に戻す。

【0008】このようにWMRパーティションが最初にウイルス・フリーであるとすれば、WMRパーティションは各新しいセッションの開始でウイルス・フリーとなる。

【0009】前記記憶媒体上のブート・パーティションは、好ましくは、被保護WMRとなる。一般パーティションは、ユーザがこれを要求するのであれば、被保護WMRともなり得る。

【0010】これを達成するために本発明の第1の特徴による方法の基本は、WMRパーティションに記憶されたオリジナルの情報を変更することなく、保持する機構を設定することであり、かつ通常これに重ね書きするデータが残りのセッション中に必要に従って、アクセスすることができる前記記憶媒体上のどこかに安全に記憶される。前記機構は、最小の付加的なメモリ空間及びスループット時間における最小の短縮と同時に、最大の安全性を提供する観点から、どのようにしてこれを効率的に行うのかを定義するものである。

【0011】本発明の第1の特徴による方法によれば、好ましくは、前記コンピュータ・システムの中央処理装置（ＣＰＵ）から独立し、かつそのユーザにアクセス不能にされたスーパバイザ手段（スーパバイザ）が設けられ、前記管理手段は、セクタから読み出されるか又はセクタに書き込まれる情報がオペレーティング・システム情報であるか又はユーザ情報であるか、前記セクタが前記ブート・パーティションであるか又は一般パーティションであるか、及び前記パーティションは活性であるか又は不活性であるかに従って、前記記憶媒体上での読み出し／書き込み動作を許可し／規制し／禁止し、前記管理手段は、活性な一般パーティション上でのみのフォーマット動作を許可し、かつ前記ブート・パーティション上で又は不活性な一般パーティション上でフォーマット動作を禁止し、かつ、禁止された読み出し、書き込み又はフォーマット動作を実行したときはユーザに警告を発生させる。

【0012】空間は、好ましくは、専用領域2と呼ばれるスーパバイザによってのみアクセス可能される前記記憶媒体上の確保する。この専用領域は特殊パーティション、WMRパーティション内のある範囲のセクタ、又は休止パーティション内の未割り付けセクタであってもよい。

【0013】各WMRパーティションは、これに関連したセクタ再割り付けテーブル（ＳＲＴ）を有し、前記テーブルを前記スーパバイザのランダム・アクセス・メモリ（ＲＡＭ）に保持し、ＳＲＴにおける各エントリは更新されたWMRパーティションにおけるある範囲のセクタのアドレスと、前記更新情報が位置するアドレスと、前記更新情報を位置決めするアドレスとを定義し、その位置が前記専用領域内にある。

【0014】本発明の第2の特徴によれば、コンピュータ・システムの記憶媒体に記憶された情報に対するアクセス及び変更を制御する装置が設けられ、前記記憶媒体はブート・パーティション及び少なくとも一つの一般パーティションを含む複数の非重複パーティションに分割された装置において、前記パーティションのうちの少なくとも一つは多数回復可能書き込み（WMR）を備え、使用中に、もし書き込みコマンドが前記WMRパーティションに記憶されている任意の情報に重ね書き（更新）するように発行されたときは、残りのセッション中の要求に従って前記更新情報をアクセスするように、前記更新情報を前記記憶媒体上の他の位置に記憶し、かつ前記更新情報に対するポインタを保持し、システム・リセットは前記更新情報を前記更新情報に対するポインタのリストと共にクリアさせ、従って非スーパバイズド・モードにより構築された際にWMRパーティションをそのオリジナルの状態に戻す装置が提供される。

【0015】前記装置は、好ましくは、前記コンピュータ・システムの中央処理装置（ＣＰＵ）から独立し、かつユーザにアクセス不能にされたスーパバイザ手段（スーパバイザ）を備え、前記管理手段は、セクタから読み出される又はセクタに書き込まれる情報がオペレーティング・システム情報であるか又はユーザ情報であるか、

前記セクタが前記ブート・パーティションであるか又は一般パーティションであるか、及びもし前記パーティションが一般パーティションであれば、前記パーティションは活性であるか又は不活性であるかに従って、前記記憶媒体上での読み出し及び書き込み動作を許可し、規制し、又は禁止し、前記管理手段は、更に、活性となる一般パーティション上のみでのフォーマット動作を許可し、かつ前記ブート・パーティション上又は不活性な一般パーティション上でのフォーマット動作を禁止し、前記監視手段は、禁止された読み出し、書き込み又はフォーマット動作であって、前記スーパバイザにより阻止されている前記動作を実行するために試行したのであれば、ユーザに警告を発生させる。

【００１６】本発明の第３の特徴によれば、コンピュータ・システムの一部を形成する記憶媒体上に記憶された情報に対するアクセス及び変更を制御する方法であって、前記記憶媒体上に記憶された情報をブート・パーティション及び少なくとも一つの一般パーティションを含む複数の非重複パーティションに分割する方法において、前記パーティションのうちの少なくとも一つを多数回復可能書き込み（ＷＭＲ）に指定し、使用中に、もし書き込みコマンドを実行する前に、前記書き込みコマンドがある又は前記ＷＭＲパーティションに記憶されている任意の情報に重ね書きするように発行された場合に、要求されたとき、例えばシステム・リセットのときに、前記情報を前記記憶媒体上の他の位置にコピーすると共に記憶して前記ＷＭＲパーティションにコピーして復帰させる方法が提供される。

【００１７】本発明の第３の特徴によれば、セッション中は制限なしに、ブート・パーティションのような前の「読み出し専用」パーティションに書き込みが許可されることは、明らかである。しかし、新しいセッションの開始時に、パーティションに対する全変更を行わず、パーティションはそのオリジナルの状態に復帰させる。従って、このパーティションを多数回復可能書き込み（ＷＭＲ）パーティションと呼んでもよい。このようにパーティションがウイルス・フリーで開始する限り、新しいそれぞれのセッションの開始でウイルス・フリーとなる。

【００１８】これを達成するために本発明の第３の特徴の方法における基本は、重ね書きされるべきＷＭＲパーティションにおける任意の「クラスタ」のコピーも前記記憶媒体上のどこかに安全に記憶され、かつ必要なときはコピーにより戻すことができる構成が設定される。この構成は、最小の付加的なメモリ空間及びスループット時間における最小の短縮と同時に、最大の安全を提供する観点においてどのようにしてこれを効率的に行うのかを定義する。

【００１９】本発明の第３の特徴の方法によれば、好ましくは、前記コンピュータ・システムの中央処理装置（ＣＰＵ）から独立して、セクタ内に記憶された情報の型式、及び前記セクタが配置されている前記パーティションの型式及びステータスに従って動作を許可する、規制する又は阻止するように、前記記憶媒体に記憶された情報に基づく読み出し、書き込み及びフォーマット動作の実行を制御する管理手段（スーパバイザ）が提供され、前記監視手段は、禁止された読み出し、書き込み又はフォーマット動作を実行するために試行したのであれば、前記コンピュータ・システムのリセットを要求させて、前記リセットはメモリをクリアさせ、かつオペレーティング・システムをロードさせる方法が提供される。

【００２０】前記記憶媒体は、特殊パーティション（ウイルス隔離空間）を備え、各ＷＭＲパーティションはファイル割り付けテーブル（ＦＡＴ）が割り付けられ、このテーブルは前記特殊パーティションに保持され、ＦＡＴにおける各エントリは前記ＷＭＲパーティションにおいて変更されたクラスタのアドレス、及び前記クラスタにオリジナルに保持された前記情報のコピーの前記アドレスを定義する。

【００２１】前記クラスタにオリジナル保持された情報は前記特殊パーティションにコピーされてもよい。

【００２２】代わって、前記クラスタにオリジナルに保持された前記情報は不活性パーティションにコピーされてもよい。

【００２３】本発明の第４の特徴によれば、コンピュータ・システムの記憶媒体に記憶された情報に対するアクセス及び変更を制御する装置であって、前記記憶媒体はブート・パーティション及び少なくとも一つの一般パーティションを含む複数の非重複パーティションに分割されている装置において、前記パーティションのうちの少なくとも一つは多数回復可能書き込み（ＷＭＲ）パーティションを備え、使用において、もし書き込みコマンドが前記書き込みコマンドを実行する前に、一つの又は前記ＷＭＲパーティションに記憶された任意の情報を重ね書きするように発行されたときは、前記情報はコピーされると共に前記記憶媒体のどこかに記憶されて、必要なときに、例えばシステム・リセットにより、前記ＷＭＲパーティションにコピーにより戻される装置が提供される。

【００２４】更に、前記装置は、好ましくは、前記コンピュータ・システムの中央処理装置（ＣＰＵ）から独立し、セクタ内に記憶された情報の型式、前記セクタが配置されている前記パーティションの型式及びステータスに従って動作を許可する、規制する又は阻止するように、前記記憶媒体上に記憶された読み出し、書き込み又はフォーマット動作の実行を制御する監視手段（スーパバイザ）を備え、使用において、前記監視手段は、禁止された読み出し、書き込み又はフォーマット動作を実行するために試行されたならば、前記コンピュータ・システムのリセットを要求させる。

【００２５】本発明の特徴による以上の方法のうちのいずれかにより、読み出し動作が前記ブート・パーティションにおける任意の情報について許可され、前記ブート・パーティションに対する書き込み又はフォーマットの試行がシステム・リセットを発生させることができる。

【００２６】更に、前記記憶媒体の複数のセクタは、前記記憶媒体のオペレーティング・システムにより定義される前記ブート・パーティションの開始セクタの位置に無関係に、前記ブート・パーティションの一部であるとみなしてもよい。

【００２７】また、活性な一般パーティションにおける任意のオペレーティング・システム情報セクタ又はユーザ発生の情報セクタの読み出しが許可され、このようなユーザ発生の情報セクタに対する書き込みが許可され、かつこのようなオペレーティング・システムの情報セクタに対する書き込みが前記パーティションの大きさ及び境界を変更するための試行がシステム・リセットを発生させるように、規制されてもよい。

【００２８】不活性な一般パーティションのオペレーティング・システム・セクタから情報を読み出すことのみが許可され、このようなパーティション上の他の読み出し、書き込み又はフォーマット動作を実行するための試行は、否定できるようにされる、又はシステム・リセットを発生させてもよい。

【００２９】読み出し、書き込み及びフォーマット動作の実行の規制又は阻止は、記憶媒体のセット・アップ又は保守できるように解除され、かつその後に再復帰にさせることができる。

【００３０】前記記憶媒体はハード・ディスク、フロッピー・ディスク、光ディスク又はテープのうちの一つから選択されてもよい。

【００３１】代わって、記憶媒体はファイルサーバであってもよく、前記コンピュータ・システムはローカル・エリア・ネットワークであり、かつユーザ・コンピュータが禁止された動作を実行するための試行が前記ユーザ・コンピュータのリセットを発生させるように、そのユーザ・コンピュータが前記ファイルサーバのどのパーティションを決定できるのかを使用している。

【００３２】本発明の以上の特徴のいずれかにより、前記装置は前記コンピュータ・システムに関連するように適応されたハードウエア手段を備えてもよい。

【００３３】代わって、前記装置は前記コンピュータ・システムに関連するように適応されたハードウエア手段を備えてもよい。

【００３４】代わって、前記装置は前記コンピュータ・システムに関連するように適応されたハードウエア手段とファームウエアとの組み合わせを提供することができる。

【００３５】ユーザ及びどのようなウイルスにもアクセス不能にされ、かつ前記記憶媒体又はその制御のもとに置かれた記憶媒体の副分割の間及び内における全てのデータ転送を監視するプロセッサを提供することもできる。

【００３６】ここで、添付図面を参照して本発明の実施例を単なる例として説明する。

【００３７】

【発明の実施の形態】本発明のセット・アップ及び動作は、含まれている種々の動作段階を説明することにより最も良く理解される。以下説明する本発明の実施例は、便宜的に、ＰＣＴ／ＧＢ／００２６１において既に開示された型式のスーパバイザを含む。従って、ここでのＰＣＴ／ＧＢ／００２６１（ＷＯ９１／１３４０３）は引用により関連される。

【００３８】まず図１及び図２の第１の実施例を参照する。

【００３９】１．１　初期接続

記憶媒体１（例えばハード・ディスク）は、まずコンピュータ・システム（図示なし）に接続され、記憶媒体１上でユーザにアクセス不能な、即ち専用領域である空間が予約されている。

【００４０】パスワードが入力されて専用領域２にか又はスーパバイザ・フラッシュＲＯＭ（図４、１３）に記憶される。このパスワードは後でコンピュータ・システムをアンスーパバイズド・モードに設定できるようにするために用いられる。

【００４１】１．２　アンスーパバイズド・モード

このモードに入るためには、アンスーパバイズド・モード・パスワードの使用が必要である（参照文献ＰＣＴ／ＧＢ／００２６１）。コンピュータ・システムがこのモードにあるときは、ユーザによりデフォールト・パーティション機構が再構築し得ても、これが提供される。

【００４２】（ａ）デフォールト機構は、典型的には、以下のパーティション型式：読み出し専用（ＲＯ）、多数回復可能書き込み（ＷＭＲ）３及び「一般」４からなる。一般パーティションは、単なるＲＯ又はＷＭＲパーティション、及び書き込み得るもの以外のパーティションである。一般パーティションは、要するに、ＲＯ若しくはＷＭＲパーティション、及び書き込みできるもの以外のパーティションである。各ＷＭＲパーティションはこれに関連され、スーパバイザＲＡＭ（図４、１４）に保持されるセクタ再配置テーブル（ＷＭＲ－ＳＲＴ）を有する。使用において、ＷＭＲ－ＳＲＴにおける各エントリは、ＷＭＲパーティション内におけるセクタ範囲のアドレスを定義し、かつ更新されたセクタの前記範囲に対するポインタを含む。各パーティションは一般パーティションに基づいたデフォールト・パーティション型式が割り付けられてもよい。例えば、パーティションＣ＝ＷＭＲ；パーティションＤ＝ＲＯ；その他の全パーティション＝一般；これらのパーティション・ラベルにより与えられるパーティション記述子。

【0043】（b）ユーザはその内容を定義する各パーティションに対する記述ストリングを定義することができる。

【0044】（c）本発明は、ユーザが（a）及び（b）を改定したい、及びパーティションを付加したい、パーティション境界を変更したい、及び各パーティションに対するパーティション型式を定義したいのであれば、ユーザを許可する。

【0045】1．3．スーパバイズド・モード

（a）スーパバイズド・モードにおけるセッションの終りでユーザが電源を断にすると、WRM－STRが無視され、更新されたセクタに対する全てのポインタを除去することは重要なことである。空のWRM－STRはWMRパーティションをそのオリジナルの状態に復帰させる。これは、コンピュータ・システムがアンスーパバイズド・モードにあったときに、最後の変更を実行した後のWMRパーティション状態を反映している。

【0046】（b）WRM－STRは使用のためにレディー（準備完了状態）に初期化される。

【0047】（c）パーティション境界及びパーティション数は、専用領域2か又はスーパバイザ・フラッシュ読み出し専用メモリ（図4、13）に記憶されているテーブルに対してチェックされる。アンスーパバイズド・モードにおいて、ユーザがこのテーブルを再構築することなくパーティションの構成を変更したときは、これを修正するまで、スーパバイズド・モードを拒絶することができる。代わって、ユーザがスーパバイズド・モードに入る度に、ユーザの介入を必要とすることない機構を用いて、テーブルを発生させることができる。

【0048】（d）ユーザは一般パーティションのリストから通常の読み出し及び書き込みのためにパーティションを選択するようにプロンプトされる。これはオペレーティング・システム及び記憶媒体1の動作の前に実行される。選択されたパーティションは「活性パーティション」として定義され、かつ残りの一般パーティションは「休止」パーティションと定義される。活性パーティションは、セッションが終了するまで、活性であり続ける。新しいセッションは、ユーザがコンピュータ・システムをリセットし、システムRAMをクリアすることにより、スーパバイズド・モードに再び入れば、再スタート可能にされる。

【0049】（e）セッションの開始で以上に対する更新として、ユーザはユーザ名、又は専用領域2におけるデータと比較できるパスワードを提供するようにプロンプトされてもよい。その際に、ユーザは活性パーティションを選択できる一般パーティションのサブセットに規制されてもよい。

【0050】（f）ユーザは全てのWMR及びROパーティション（勿論、選択された活性パーティション）に対して完全なアクセスが与えられている。

【0051】4．WMRパーティションに対するアクセス

既に述べたように、WRM－STRは、各WMRパーティション3について定義され、かつ専用領域2に記憶されていた。

【0052】（a）本発明の動作中に、WMRパーティション3におけるセクタの範囲は、更新する必要があるものであってもよい。これが発生すると、スーパバイザ（図示なし）は、更新されるべきセクタの範囲を定義し、かつ前記更新したセクタを書き込む（専用領域における）位置に対するポインタをセットしたWRM－STRにおけるエントリを発生する。変更されていないオリジナルのセクタは、そのオリジナルの位置にある。

【0053】（b）更新されたセクタは専用領域内の記憶媒体におけるどこかに記憶されてもよい。この専用領域は特殊パーティションであってもよい。代わって、専用領域は休止パーティション内に配置されていてもよい。セッション中はユーザが休止パーティションをアクセスすることはできないので、新しいセッションが開始される前に解除することができる未割り付けセクタを使用するのが安全である。これを図1に示す。

【0054】（c）スーパバイザは、WMRパーティション3に書き込むために要求を出すときは、図2に示すフローチャートに従う。

【0055】（d）スーパバイザは、WMRパーティション3から読み出すために要求を出すときは、図2に示すフローチャートに従う。

【0056】（e）前記パーティションに対する書き込み動作がその書き込み動作を完了させる前に、オリジナルのセクタを安全位置にコピーさせるWMRパーティションを実行する他の機構が可能である。各セッションの開始で、オリジナルのセクタがWMRパーティション内のオリジナルの位置にコピーにより戻され、前記パーティションをそのオリジナルの状態に復帰させる。

【0057】ここで、図4及び図5の第2の実施例に戻る。

【0058】2．1．初期接続

記憶媒体101（例えばハード・ディスク）がまずコンピュータ・システム（図示なし）に接続されると、ユーザにアクセス不能となる空間が記憶媒体101上に予約される。この空間は特殊パーティションであり、これをウイルス隔離空間102と呼ぶことができる。

【0059】パスワードがウイルス隔離空間2に入力されて記憶される。このパスワードは後にコンピュータ・システムをアンスーパバイズド・モードに設定させるために使用される。

【0060】2．2　アンスーパバイズド・モード

このモードはアンスーパバイズド・モードのパスワードを必要とする（参照文献PCT／GB／00261）。システムがこのモードにあるときは、ユーザはコンピュ

ータ・システム及びウイルス隔離空間１０２の両方を構築することができる。

【００６１】（ａ）ユーザは、各パーティションに対して、そのパーティションを読み出し専用（ＲＯ）（図示なし）にするのか、多数回復可能書き込み（ＷＭＲ）１０３にするのか、又は「通常」１０４にするのかを定義することができる。一般パーティションは、単純にＲＯ又はＷＭＲパーティション以外のパーティション、及び書き込みができるものである。各ＷＭＲパーティションは、これに割り付けられ、ウイルス隔離空間１０２に保持されるファイル割り付けテーブル（ＷＭＲ－ＦＡＴ）を有する。使用において、ＷＭＲ－ＦＡＴにおけるエントリはウイルス隔離空間１０２に保持される。使用において、ＷＭＲ－ＦＡＴにおける各エントリはＷＭＲパーティション内で変更されたクラスタのアドレスを定義し、かつ変更されていないオリジナルのクラスタのコピーに対するポインタを含む。

【００６２】（ｂ）ユーザは各パーティション用の記述ストリングを定義して、その内容を定義することができる。

【００６３】（ｃ）パーティションが付加された、又は境界が変更されたときは、ユーザは（ａ）及び（ｂ）を改定することができる。ユーザがコンピュータ・システムによりこれを実行するように強制されないときは、「一般」ステータス及び「パーティション１０４′」のようなデフォールトが採用される。

【００６４】一般的な一定のガイドラインが設けられているのであれば、機構はユーザの介入なしに作動するので、必要される正確なハウスキーピングは定義する必要はない。例えば、パーティションＣ＝ＷＭＲ；他の全てのパーティション＝通常；これらのドライブ文字により与えられたパーティション記述子。

【００６５】２．３　スーパバイズド・モード

（ａ）全てのＷＭＲパーティション１０３は、ウイルス隔離空間１０２におけるＷＭＲ－ＦＡＴを参照することにより、それらのオリジナルの状態に復帰される。これは、整合性のために、アンスーパバイズド・モードに入ったときにも発生する。

【００６６】各ＷＭＲ－ＦＡＴエントリはＷＭＲパーティション１０２内の変更クラスタ（即ちそのアドレス）に対するポインタ、及びオリジナルのクラスタのコピーに対するポインタを含む。従って、各セッションの開始において、以下の手順は、全てＷＭＲパーティション１０２を復帰させるために必要とされるものである。

各ＷＭＲ－ＦＡＴエントリに対して：

－オリジナルのクラスタをＷＭＲパーティション１０２における位置にコピーする（図１に示すように、クラスタ「Ｘ」をクラスタ「Ａ」にコピーする）。

－ＷＭＲ－ＦＡＴエントリを削除する。

（注：このシーケンス中の電源断又はシステム・クラッシュは、手順を反復させる必要があるかも知れないが、オリジナルのＷＭＲパーティションを復帰させる機能には影響しない。）

【００６７】（ｂ）ＷＭＲ－ＦＡＴ（又は複数のＷＭＲ－ＦＡＴ）は初期化されて使用レディーとなる。

【００６８】（ｃ）パーティション境界及びパーティション数はウイルス隔離空間１０２に記憶されたテーブルに対してチェックさせる。アンスーパバイズド・モードにおいて、ユーザがウイルス隔離空間１０２を再構成することなく、パーティションの構成を変更したときは、これを修正するまで、スーパバイズド・モードを拒絶することができる。

【００６９】（ｄ）ユーザは一般パーティションのリストから通常の読み出し及び書き込みのためにパーティションを選択するようにプロンプトされる。これはオペレーティング・システム及び記憶媒体１０１の動作の前に実行される。選択されたパーティションは「活性パーティション」として定義され、かつ残りの通常パーティションは「休止」パーティションと定義される。活性パーティションは、セッションが終了するまで、活性であり続ける。新しいセッションは、ユーザがシステムＲＡＭをクリアし、コンピュータ・システムをリセットすることにより、スーパバイズド・モードに再び入ると、再スタート可能にされる。

【００７０】（ｅ）セッションの開始で以上に対する更新として、ユーザはユーザ名、又は専用領域１０２におけるデータと比較できるユーザ名又はパスワードを提供するようにプロンプトされてもよい。そのときに、ユーザは活性パーティションを選択し得る通常パーティションのサブセットに規制されてもよい。

【００７１】（ｆ）ユーザは全てのＷＭＲ及びＲＯパーティション（勿論、選択された活性パーティション）に対して完全なアクセスが与えられている。

【００７２】４．ＷＭＲパーティションに対するアクセス

既に述べたように、ＷＲＭ－ＳＴＲは、各ＷＭＲパーティション１０３について定義され、かつ専用領域１０２に記憶されていた。

【００７３】（ａ）本発明の動作中に、ＷＭＲパーティション１０３におけるクラスタは、更新が必要されるものでもよい。これが発生すると、スーパバイザ（図示なし）は、更新しようとするクラスタを定義し、かつ前記オリジナルのコピーに対するポインタを有するＷＲＭ－ＳＴＲにおけるエントリを発生する。

【００７４】（ｂ）オリジナルのクラスタのコピーは記憶媒体におけるどこかに記憶されてもよい。例えば、これは特殊パーティション又はウイルス隔離空間１０２における領域のようにその目的のために予約された専用領域に記憶されてもよい。代わって、オリジナル・クラスタは休止パーティション内の一時的な空間に見い出すこ

とができる。セッション中にユーザ（従ってウイルス）が休止パーティションをアクセスすることはできないので、オリジナル・クラスタが安全であり、かつ新しいセッションが開始される前に解除されてもよい。これを図1に示す。

【0075】（c）スーパバイザは、WMRパーティション103に書き込み要求が出されると、図2に示すフローチャートに従う。

【0076】ここで図6を参照すると、本発明の実施例において用いるスーパバイザの第1の実施例を実行するのに適したハードウエア構成のブロック図が示されている。このスーパバイザはパーソナル・コンピュータ（PC）等のマザー・ボードに対する典型的なバス・インターフェイス7と、各セッションの開始時にモード・エントリを制御するように適当なBIOS（基本入出力システム）を含む読み出し専用メモリ（ROM）とを備えている。

【0077】スーパバイザはPCのディスク・インターフェイスとディスク・ドライブとの間に存在するように設計される。PCはその集積デバイス・エレクトロニックス（IDE）バスからリボン・ケーブル201を介してスーパバイザに接続される。次いで、スーパバイザは、IDEバスとしても機能する第2のリボン・ケーブル202を介してディスク・ドライブと接続される。PCとハード・ディスクとの間の全ての通信は、スーパバイザにより制御される。

【0078】スーパバイザ・ハードウエアは、マイクロプロセッサ216と、スーパバイザ・オペレーティング・システム及び制御プログラムを保持している読み出し専用メモリ（ROM）213と、パラメータ及びWRM－SRT（又は複数のSRT）を保持するために用いられるスクラッチ・メモリであるランダム・アクセス・メモリ（RAM214）とを備えている。

【0079】二重ポートRAM210は、PC及びスーパバイザ・プロセッサの両者がアクセスすることができるメモリを備えている。スーパバイザはIDEタスク・レジスタを反映させるためにこのメモリを用いてもよい。

【0080】トランシーバ206、209及びマルチプレクサ205は、PC又はスーパバイザ・プロセッサにディスク・ドライブをアクセスするのを許可する。スーパバイザは、これらのうちのいずれがアクセスを有するのかを制御する。ラッチ207、208は、8ビット・バスを有するスーパバイザにディスク・ドライブから16ビット値を読み出せるように、かつ書き込めるようにする。

【0081】ロジック・ブロック212はスーパバイザ・プロセッサにより書き込み可能とされるラッチを含む。このラッチの値はPCインターフェイス・アッパー・アドレス・バスと比較され、またBIOS211はこれらが一致したときにのみ、イネーブルにされる。これはBIOSをスーパバイザを介して構築させ、最低メガバイトのPCアドレス空間における任意の位置に出現させる。

【0082】ロジック・ブロック215は、ROM213、RAM214及び二重ポートRAM210をスーパバイザ・プロセッサ・アドレス空間にマップさせる。このロジック・ブロック215は、更に、ラッチ207、208及びロジック・ブロック212内に対するアクセスも制御している。

【0083】ロジック・ブロック204は、PCとディスク・ドライブとの間を通過する制御信号が正しくバッファされ、かつスーパバイザ・プロセッサがディスク・ドライブに接続されているときに、これらの制御信号を禁止するのを保証している。

【0084】ロジック・ブロック203は、PCとディスク・ドライブとの間の通信がスーパバイザの制御に従うことを保証している。これはディスク・ドライブ上のタスク・ファイル・レジスタに対する読み出しコマンド及び書き込みコマンドを監視すると共に制御する。スーパバイザ・プロセッサは試行している臨界的な動作を認識するようにされて、動作が進行しているか、阻止されているか、又は要求が変化したかを制御している。これは、読み出し制御信号及び書き込み制御信号と共に、PCアドレス・ラインをデコードすることにより実行される。一定の読み出し及び書き込みの試行により、スーパバイザ・プロセッサの割り込みを発生させることになる。そこで、スーパバイザは変化に基づいて作動する。複数のディスク・ドライブ割り込みは、まずスーパバイザ・プロセッサに導かれて、そこで必要によりPCに転送することもできる。

【0085】スーパバイザ・プロセッサ216は内蔵するROM213から実行可能なコードをフェッチすることのみが可能なので、図4を調べることによりウイルスがスーパバイザ・プロセッサ216を妨害することは決してあり得ないことが明確になる。

【0086】ここでは図6に示すスーパバイザの実施例の更に詳細な説明はしないが、これは当該技術分野に習熟する者が通常に理解する範囲内にあるからである。

【0087】ここで図7を参照すると、本発明の第2の実施例を実行するために適当なハードウエア構成のブロック図が示されている。このスーパバイザは、パーソナル・コンピュータ（PC）等のマザーボードに対する典型的なハード・ディスク・アダプタ・カード・インターフェイス310と、ハード・ディスクを動作させるために適当なBIOS（基本入出力システム）を含む読み出し専用メモリ（ROM）312と備えている。

【0088】スーパバイザ・ハードウエアはマイクロプロセッサ314及びトランシーバ316を含み、PCが複数のディスク・ドライブのために直接的な選択、又は

アービトレーションを行うこと、又はＳＣＳＩインターフェイス３１８を介してコマンドを発行することができないように、ＳＣＳＩ３１８に対するＰＣ規制のアクセスを許可する。これらの動作は、ステータス入出力ポート３２０及び３２２を用いて、ＰＣと双方向に通信するスーパバイザ・プロセッサ３１４によってのみ実行することができる。

【００８９】スーパバイザ・プロセッサ３１４とＳＣＳＩインターフェイス３１８との間の通信は第２のトランシーバ３２４の双方向ポートを介して行われる。スーパバイザは、更に、スーパバイザ・オペレーティング・システム及び制御プログラムを含む内蔵する読み出し専用メモリ（ＲＯＭ）３２６と、パラメータを保持するために用いられるスクラッチ・メモリであるランダム・アクセス・メモリ（ＲＡＭ）３２８とを備えている。リセット・ロジック３３０が更に設けられており、もしスーパバイザにより禁止されている動作を実行しようとしたときは、ＰＣメモリをクリアするために用いられる。

【００９０】図８を参照すると、図７のものと同一番号による整数により、スーパバイザの実施例の概要ブロック図が示されている。

【００９１】更に、図８の実施例は、次の構成要素：ゲート・アレー・ロジック（ＧＡＬ）デバイスＧ１～Ｇ５；バッファＢ１、Ｂ２；及びフリップ・フロップ７４、１（１）、７４、１（２）及び７４、２（２）を備えている。

【００９２】この構成要素の機能は次のようである。Ｇ１は、ＲＯＭ　ＢＩＯＳをＩＢＭメモリ・マップにマップさせ、更に、ＩＢＭデータ・バスに対するフリップ・フロップ７４、２（２）の出力のトライステート接続を行う。

【００９３】Ｇ２は、ＩＢＭによるＳＣＳＩコントローラの内部レジスタのサブセットに対するアクセスを、これらをＩＢＭ　Ｉ／Ｏ空間にマッピングすることにより行う。Ｇ２は、更に、ＳＣＳＩコントローラへ又はからのデータ転送をするための疑似ＤＭＡデコーディング・ロジックとなり、かつフラグ即ちフリップ・フロップ７４、２（２）及びＰ１をＩＢＭ　Ｉ／Ｏ空間にマップさせる。

【００９４】Ｇ３は、スーパバイザ・バスとＩＢＭアドレス・バスとの間をＳＣＳＩコントローラ・アドレス・バスへ多重化させる。

【００９５】Ｇ４は、スーパバイザ・バスとＩＢＭ制御ラインとの間をＳＣＳＩコントローラへ多重化させる。Ｇ４は、更に、トランシーバＴ１又はＴ２（両者ということは絶対ない）をイネーブルすると共に、ＩＢＭとＳＣＳＩコントローラとの間でのデータ転送中に可能ウエイト・ステート用のロジックを備えている。

【００９６】Ｇ５は、スーパバイザ入出力空間における全てのポート、即ちラッチＰ１、Ｐ２、ＳＣＳＩリセット・ライン及びフリップ・フロップ７４、１（２）及び７４、２（２）をマップさせる。Ｇ５は、更に、ＲＯＭをスーパバイザ・メモリ・マップにマップさせ、フリップ・フロップ７４、２（２）の出力をスーパバイザ・データ・バスへトライステート接続させる。

【００９７】バッファＢ１、Ｂ２は、ＩＢＭバックプレーンからの電流をアドレスＩＯＲ及びＩＯＷラインのそれぞれのために流し込む唯一のゲートとなり得ることを保証している。

【００９８】フリップ・フロップ７４、１（１）はクロック周波数を１／２に分周すると共にパルスを矩形波にする。ＳＣＳＩコントローラに対してＩＢＭが（規制された）アクセスを有するか、又はスーパバイザがアクセスを有するかは、フリップ・フロップ７４、１（２）の出力による。

【００９９】フリップ・フロップ７４、２（１）はＳＣＳＩデータ転送中のウエイト・ステート発生に関するタイミング形成の一部をなし、一方フリップ・フロップ７４、２（２）は、データ・バイトがＩＢＭから送出されたことを表すスーパバイザのアテンション用のフラグである。

【０１００】図４の実施例の構成要素は次のようである。ＧＡＬのＧ１～Ｇ５はＳＣＳトムソンＧＡＬ１６Ｖ８～１５ｎｓ型のものであり、フリップ・フロップ７４、１（１）、７４、１（２）、７４、２（１）及び７４、２（２）は７４ＡＬＳ７４型のものであり、バッファＢ１、Ｂ２は７４ＡＬＳ２４４であり、ラッチＰ１、Ｐ２は７４ＡＬＳ７３であり、トランシーバＴ１、Ｔ２は７４Ｆ２４５であり、プロセッサ１４はザイログＺ８４Ｃ５０（１０ＭＨｚ）であり、読み出し専用メモリ１２は２７６４（８Ｋ×８）であり、ＳＣＳＩコントローラ１８はＮＣＲ５３８０である。

【０１０１】スーパバイザ・マイクロプロセッサ３１４は内蔵するＲＯＭ３２６から実行可能なコードをフェッチすることのみが可能なので、図８を調べることによりウイルスがスーパバイザ・プロセッサ３１４を妨害することは決してあり得ないことが明確となる。

【０１０２】ここでは図８に示すスーパバイザの実施例の更に詳細に説明はしないが、これは当該技術分野に習熟する者が通常に理解する範囲内にあるからである。

【０１０３】以上、本発明の実施例は単なる例として挙げたものであって、いずれにしろ本発明の範囲を限定することを意図するものではない。

【０１０４】本発明は、記憶及びパフォーマンス・オーバーヘッドにほとんど影響することなく、これまで従来技術において顕著であった問題を除去しようとしていることを理解すべきである。本発明は「スーパバイズド」ユーザにブート・パーティションに対する完全な読み出し及び書き込みアクセスを可能にすると共に、コンピュータ・システム上で各セッション開始におけるブート・

パーティションがクリーンなウイルス・フリーであり、かつ改変されていないことを保証している。これは、以上で概説した問題に対処すると共に、ＰＣＴ／ＧＢ９１／００２６１に開示された完全なウイルス防止の維持を可能にさせる。

【０１０５】ユーザはセッション間での変化を維持したいとみなすことができる。その場合に、ユーザは、シャットダウンを行う前に、活性パーティションにおける変更ファイルを記憶するバッチ・ファイルを作成することができる。新しいセッションの開始において、これらのファイルはWMRパーティションにおけるオリジナルのものと置換することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例において用いる記憶媒体の分割を示す概略図。

【図２】コンピュータ・システムが図１の実施例に用いた多数回復可能書き込み（WMR）パーティションに書き込みをしようとするときの事象のシーケンスを示すフローチャート。

【図３】コンピュータ・システムが多数回復可能書き込み（WMR）パーティションから読み出しをしようとするときの事象のシーケンスを示すフローチャート。

【図４】本発明において用いる記憶媒体の分割を示す概略図。

【図５】コンピュータ・システムが図４の実施例において用いた多数回復可能書き込み（WMR）に書き込みをしようとするときの事象のシーケンスを示すフローチャート。

【図６】本発明において用いるスーパバイザの第１の実施例のハードウエア構成の概要ブロック図。

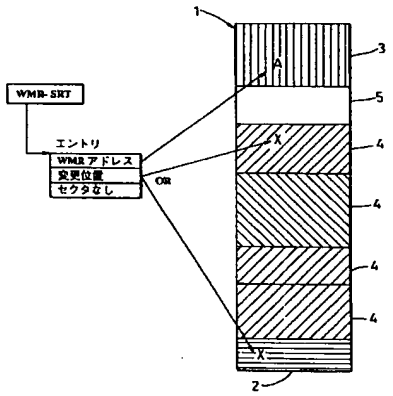
【図７】本発明において用いるスーパバイザの第２の実施例のハードウエア構成の概要ブロック図。

【図８】図７のスーパバイザの実際の実施例の概要回路図。

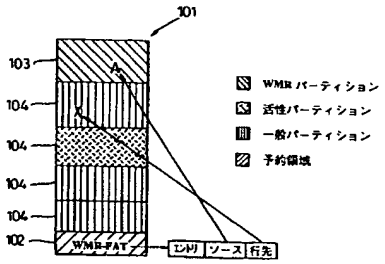
【符号の説明】

１０１　記憶媒体
１０２　ウイルス隔離空間
１０３　WMRパーティション
２１３　読み出し専用メモリ（ROM）
２１４　ランダム・アクセス・メモリ（RAM）
２１６、３１４　マイクロプロセッサ
３１８　ＳＣＳＩインターフェイス
３３０　リセット・ロジック

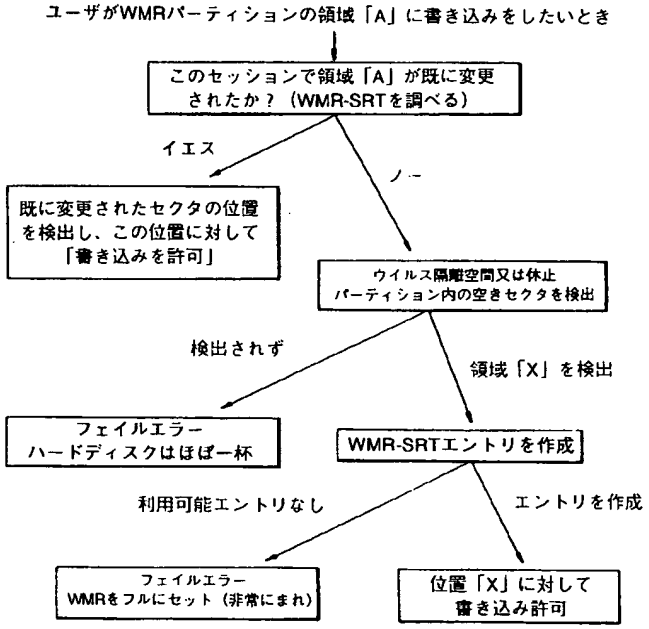
【図１】



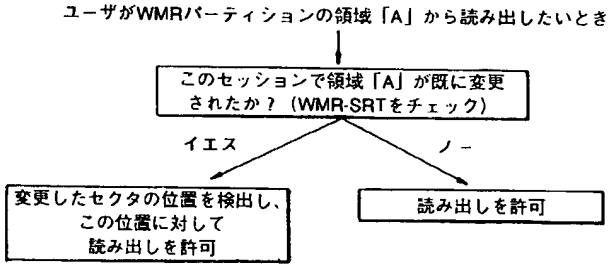
【図４】



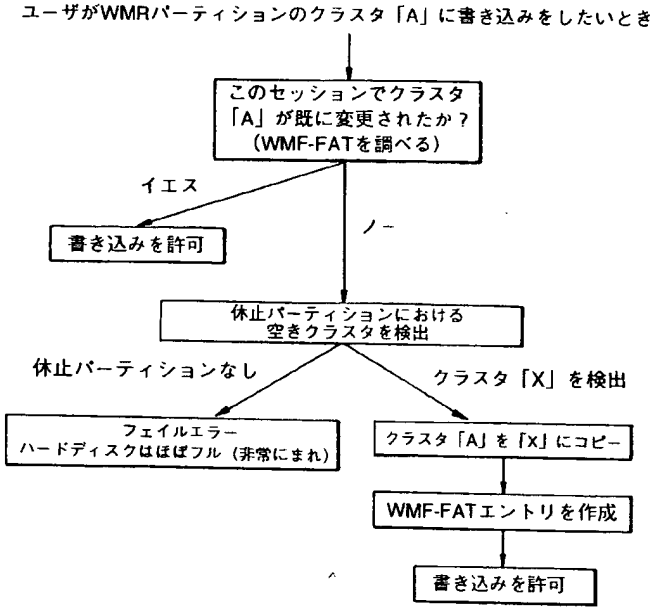
【図2】


ユーザがWMRパーティションの領域「A」に書き込みをしたいとき
このセッションで領域「A」が既に変更されたか？（WMR-SRTを調べる）
イエス
ノー
既に変更されたセクタの位置を検出し、この位置に対して「書き込みを許可」
ウイルス隔離空間又は休止パーティション内の空きセクタを検出
検出されず
領域「X」を検出
フェイルエラー
ハードディスクはほぼ一杯
WMR-SRTエントリを作成
利用可能エントリなし
エントリを作成
フェイルエラー
WMRをフルにセット（非常にまれ）
位置「X」に対して書き込み許可

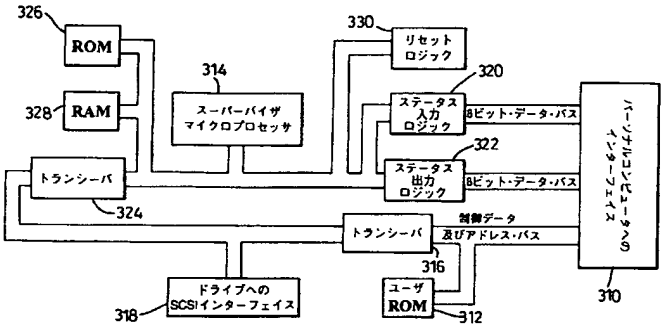
【図3】


ユーザがWMRパーティションの領域「A」から読み出したいとき
このセッションで領域「A」が既に変更されたか？（WMR-SRTをチェック）
イエス
ノー
変更したセクタの位置を検出し、この位置に対して読み出しを許可
読み出しを許可

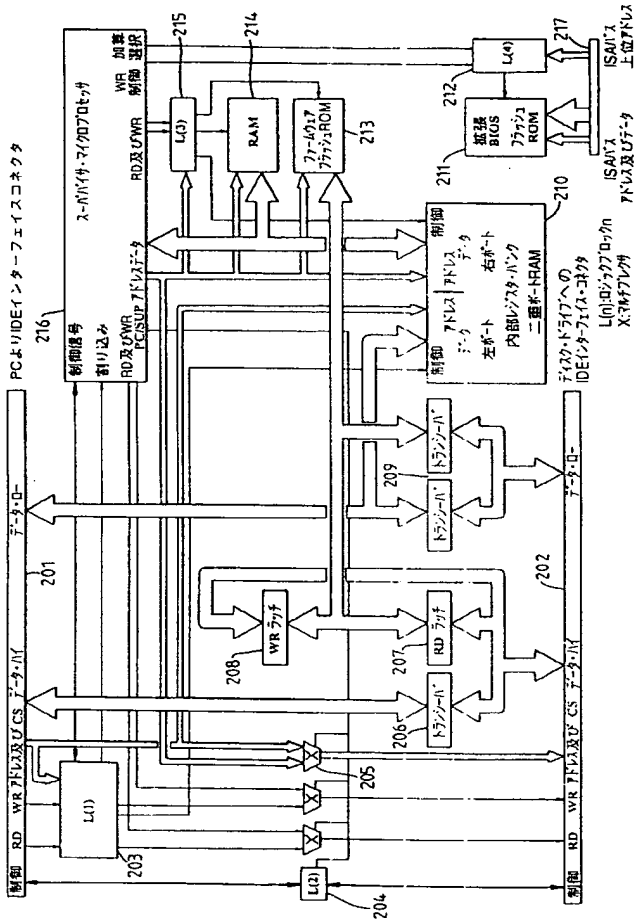
【図5】


ユーザがWMRパーティションのクラスタ「A」に書き込みをしたいとき
このセッションでクラスタ「A」が既に変更されたか？（WMF-FATを調べる）
イエス
ノー
書き込みを許可
休止パーティションにおける空きクラスタを検出
休止パーティションなし
クラスタ「X」を検出
フェイルエラー ハードディスクはほぼフル（非常にまれ）
クラスタ「A」を「X」にコピー
WMF-FATエントリを作成
書き込みを許可

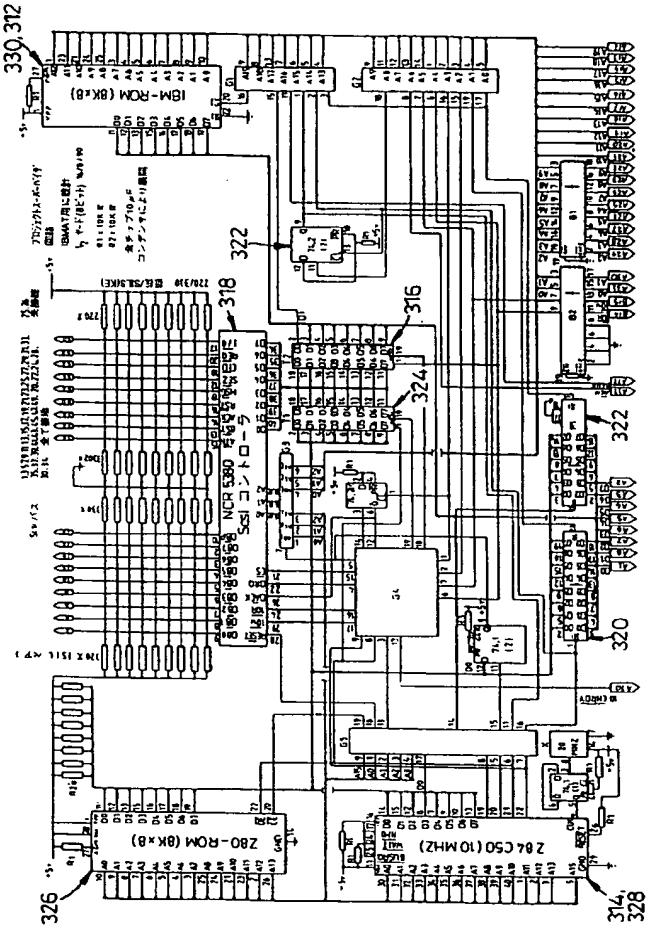
【図7】


326
ROM
328
RAM
314
スーパーバイザ マイクロプロセッサ
330
リセット ロジック
320
ステータス 入力 ロジック
8ビット・データ・バス
322
ステータス 出力 ロジック
8ビット・データ・バス
パーソナルコンピュータへのインターフェイス
トランシーバ
324
トランシーバ
制御データ及びアドレス・バス
316
ドライブへのSCSIインターフェイス
318
ユーザROM
312
310

【図6】


PCよりIDEインターフェイスコネクタ
スーパバイザ・マイクロプロセッサ
制御信号
割り込み
RD及びWR
PCSUP アドレス/データ
WR 制御
RD及びWR
加算 選択
L(3)
RAM
ファームウェア フラッシュROM
L(4)
拡張 BIOS フラッシュ ROM
ISAバス 上位アドレス
ISAバス アドレス及びデータ
制御
アドレス
データ
左ポート
右ポート
内部レジスタ・バンク
二重ポートRAM
ディスク・ドライブへの IDEインターフェイス・コネクタ
L(n):ICソケットのピン番号
X:マルチプレクサ
データ・バス
WR アドレス及び CS
RD
WR ラッチ
RD ラッチ
トランシーバ
L(1)
L(2)
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217

【図8】



フロントページの続き

(72)発明者　リジナルド　キリアン
イギリス国バーンティスランド，カークバンク　ロード　39